What is claimed is:

1. A memory protection system comprising:

a key store storing identifiers of protected memory locations and respective corresponding memory protection keys; and

a memory access manager configured to receive a memory command for altering contents of any of the protected memory locations, and for each memory command, to determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, and, where the memory command includes the memory protection key corresponding to each protected memory location to be altered, to permit the memory command and then render each memory protection key in the command inaccessible.

2. The system of claim 1, wherein the identifiers comprise addresses in a protected memory.

3. The system of claim 1, wherein the identifiers comprise names of protected files in a memory.

4. The system of claim 1, wherein the identifiers identify data entries in a protected memory.

5. The system of claim 1, wherein each of the memory protection keys comprises a modified version of a data sequence.

6. The system of claim 5, wherein the modified version comprises a hash of the data sequence.

7. The system of claim 1, wherein the key store stores a mapping table that maps each identifier to a corresponding memory protection key.

8. The system of claim 7, wherein at least one of the identifiers is mapped to multiple corresponding memory protection keys.

9. The system of claim 1, implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations.

10. The system of claim 9, wherein the memory access manager is further configured to receive memory commands for altering contents of the unprotected memory locations, and to permit the memory commands for altering contents of the unprotected memory locations and each memory command for altering contents of any protected memory location that includes the memory protection key corresponding to each protected memory location to be altered.

11. The system of claim 1, wherein the memory access manager is further configured to perform each memory command that includes the memory protection key corresponding to each protected memory location to be altered.

12. The system of claim 1, implemented in an electronic device, wherein the memory commands are received by the memory access manager from an originating electronic device component, and wherein the originating electronic device component proceeds with each memory command permitted by the memory access manager.

13. The system of claim 12, wherein the originating electronic device component is a memory update module.

14. The system of claim 12, wherein the originating electronic device component sends memory commands to the memory access manager responsive to data received at the electronic device.

15. The system of claim 14, wherein the originating electronic device component is further configured to extract a received memory protection key from the received data and to provide the received memory protection key to the memory access manager.

16. An electronic device comprising:

a memory;

a receiver configured to receive data to be written to the memory; and

a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location.

17. The electronic device of claim 16, wherein the memory comprises unprotected memory locations into which the received data is written.

18. The electronic device of claim 17, wherein each key is rendered inaccessible by erasing the received data from the unprotected memory locations where the memory access manager allows the received data to be written to the protected memory locations.

19. The electronic device of claim 16, wherein the memory protection system comprises:

a key store storing a mapping table that associates the protected memory locations with the respective corresponding keys; and

a memory access manager configured to process memory a command for writing the received data to any of the protected memory locations, to determine whether the received data includes the key corresponding to any of the protected memory locations to which the received data is to be written, and, where the received data includes the key corresponding to a protected memory location to which the received data is to be written, to permit the memory command and then render the corresponding key in the received data inaccessible.

20. The electronic device of claim 19, wherein the memory comprises a file system, and wherein the key store resides at a secure location in the memory outside the file system.

21. The electronic device of claim 16, wherein the receiver comprises one or more components selected from the group consisting of: a wireless receiver, a wireless transceiver, a modem, a network interface, a serial port, a parallel port, a Universal Serial Bus (USB) port, an infrared port, and a short-range wireless communication module.

22. A method of protecting memory in an electronic device, comprising:

receiving a memory command to alter a protected memory location;

identifying a memory protection key corresponding to the protected memory location;

determining whether the memory command includes the memory protection key corresponding to the protected memory location;

permitting completion of the memory command where the memory command includes the memory protection key corresponding to the protected memory location; and

rendering the memory protection key in the memory command inaccessible.

23. The method of claim 22, wherein permitting comprises performing the memory command.

24. The method of claim 22, wherein receiving comprises receiving the memory command from an originating electronic device component, and wherein permitting comprises allowing the originating electronic device component to perform the memory command.

25. The method of claim 22, further comprising:

receiving data to be written to the protected memory location; and

generating the memory command responsive to receiving the data.

26. The method of claim 25, wherein the received data comprises a received key, and wherein generating comprises extracting the received key from the received data and inserting the received key into the memory command.

27. The method of claim 26, wherein determining comprises comparing the memory protection key corresponding to the protected memory location with the received key in the memory command.

28. The method of claim 26, wherein determining comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location.

29. The method of claim 25, further comprising the step of:

storing the received data to an unprotected memory location,

wherein rendering the memory protection key in the memory command inaccessible comprises erasing the received data from the unprotected memory location upon completion of the memory command.

30. The method of claim 22, wherein identifying comprises identifying a protected memory location in the memory command and accessing a mapping table that maps protected memory locations to respective corresponding memory protection keys.

31. The method of claim 22, wherein the memory command comprises one of a memory write command and a memory erase command.

32. The method of claim 22, further comprising:

receiving memory commands to alter unprotected memory locations; and

permitting completion of the memory commands to alter unprotected memory locations.

33. The method of claim 22, further comprising:

receiving memory read commands; and

permitting completion of the memory read commands.

34. The method of claim 22, wherein said identifying step comprises accessing the memory protection key corresponding to the protected memory location in a key store, the method further comprising:

receiving a command to establish a new protected memory location in the memory and a memory protection key corresponding to the new protected memory location;

establishing the new protected memory location in the memory; and

storing the memory protection key in the key store.

35. A computer-readable medium storing instructions for performing the method of claim 22.

36. A method of protecting electronic memory, comprising:

configuring a memory store of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key; and

configuring a processor of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location, and for at least one memory command, to determine whether the memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said memory command including the memory protection key corresponding to at least one said protected memory location to be modified, to permit the memory command and then render each corresponding memory protection key in the command inaccessible.

37. The method of claim 36, wherein the memory store comprises the protected memory locations and unprotected memory locations.

38. The method of claim 36, wherein configuring the processor comprises installing memory access manager software on the electronic device for execution by the processor.

39. A computer-readable medium storing instructions for performing the method of claim 36.

40. A computer-readable medium storing instructions for performing the method of claim 38 and the memory access manager software.